UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of
Information associated with
kennyshelton2450@gmail.com

Case No: MJ-22-860-STE

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252	Possession and distribution of child pornography

The application is based on these facts:

See attached Affidavit of Special Agent Austina Blecha, Office of Special Investigations , which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Austina Blecha
Special Agent
Office of Special Investigations

Sworn to before me and signed in my presence.

Date: Nov 29, 2022

Judge's signature

City and State: Oklahoma City, Oklahoma

Shon T. Erwin, U.S. Magistrate Judge
Printed name and title

THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Austina Blecha, a Special Agent (SA) with the Office of Special Investigations (OSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for information associated with an account that is stored at premises controlled by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.[1] The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC (Google) to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed as a Special Agent (SA) with the Office of Special Investigations (OSI) since October 2021, and I am currently assigned to OSI Detachment 114, Tinker Air Force Base (TAFB), Oklahoma. Since joining OSI, I have been involved in investigations of child exploitation matters and computer crimes against children. I currently

---

[1] On October 25, 2022, this Court issued a search warrant in case no. MJ-22-778-STE for the same subject account and based on the same probable cause detailed in this affidavit. The deadline to execute that warrant November 7, 2022. However, investigators did not serve the warrant on Google LLC by November 7, 2022. That warrant will be returned unexecuted.

investigate violations of the Uniform Code of Military Justice (UCMJ) and United States laws involving the exploitation of children where a military nexus exists. I have gained expertise in conducting such investigations through in-person trainings, classes, and everyday work in my current role as an SA with OSI. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program and the United States Air Force Special Investigations Academy, where I completed more than 600 hours of training. I possess a Bachelor of Science in Forensic Chemistry from Western Illinois University and a Master of Science in Criminal Justice from Aspen University.

3. I am investigating the online activities of Senior Airman Kenneth Michael Shelton (SHELTON), 72nd Security Forces Squadron (SFS), TAFB, OK, who resides in the Western District of Oklahoma at 3815 Shadywood Dr., Apt 413, Midwest City, Oklahoma (the SUBJECT PREMISES). As shown below, there is probable cause to believe that SHELTON used a Google account associated with the email address kennyshelton2450@gmail.com (the SUBJECT ACCOUNT) to possess child pornography in violation of 18 U.S.C. § 2252 and that evidence of that crime will be found in the SUBJECT ACCOUNT. I submit this Application and Affidavit in support of a search warrant authorizing a search of the SUBJECT ACCOUNT as further described in Attachment A. There is probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

4. I submit this affidavit based on information known to me personally from the investigation, as well as information obtained from others who have investigated this matter or have personal knowledge of the facts herein. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me

concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the foregoing violation are presently located in the SUBJECT ACCOUNT.

BACKGROUND OF THE INVESTIGATION

5. On or about 12 September 2022, OSI Center, Criminal Integration Branch, Marine Corp Base (MCB) Quantico, Virginia, provided OSI Detachment 114, TAFB, Oklahoma, with a referral of a CyberTipline Report originating from the National Center for Missing and Exploited Children (NCMEC).

6. According to NCMEC CyberTipline Reports 128344571 and 128353024, Google notified NCMEC of 23 files uploaded on July 1, 2, and 3, 2022, from the email address kennyshelton2450@gmail.com (the SUBJECT ACCOUNT) and stored on the Google Drive associated with that account. The hash values of all 23 files matched previously identified child pornography. Hash values are digital identifiers that are so unique that it is highly unlikely that two different files would ever have the same hash value. Of the 23 files, Google reviewed the entire contents of following five files:

Filename
Google-CT-RPT-ff25f68b77f3775525caa64c5dbab1e-PthcPedo-Lolita Collection-New-Clips-2016 (114).wmv
Google-CT-RPT-d7c1669eb1b75a30644d525581dbc157-!-0-AMY-(1[1].87MB-Joyfully-Sucks-COCK-Yummy(1).wmv
Google-CT-RPT-7212029b2f7795917515960c4dca6b6fpthc_pedo Niña de 12yo mama como puta polla de mierda.mpeg
Google-CT-RPT-46b91e6850998d90964bcb80beffa0d1-vlcrecord-2015-01-05-23h10m12s-(pthc) - new! - emma and her sister sara blowjobs 2010 mpeg4 avi-(4).mpg
Google-CT-RPT-b5e241afbf5efbd5993300be6d062845-xxxxxx(Lolita-Sf-1Man) Pthc - Jessie (12Yo) - Jessie Blowjob -Part 3 - [00.00.24].mpg

After reviewing the five files, Google identified them as apparent child pornography. OSI reviewed the same five files, which depict prepubescent and pubescent minor girls engaged in sexual acts with adult men.

7. The NCMEC reports identified the account owner of kennyshelton2450@gmail.com as first name Kenny and last name Shelton. The NCMEC reports included the account owner's birthdate and verified mobile phone number. According to SHELTON's Air Force personnel records, his birthday matches the birthday of the owner of the SUBJECT ACCOUNT. SHELTON's Air Force personnel records also reflect that on February 4, 2021, SHELTON listed his email as kennyshelton2450@gmail.com and listed a phone number that matches the mobile phone number associated with the SUBJECT ACCOUNT.

8. An initial query of the Department of Defense Person Search (DPS) database showed SHELTON is an active duty military member living with his wife and infant son. DPS showed that SHELTON is assigned to the 72nd Security Forces Squadron at Tinker Air Force Base, Oklahoma, and listed his residence in Oklahoma City. On September 29, 2022, OSI interviewed the First Sergeant of SHELTON's squadron, who advised that SHELTON's wife and infant son no longer live in Oklahoma. The First Sergeant advised that sometime between the middle of June and early July 2022, SHELTON moved to the SUBJECT PREMISES.

9. On October 17, 2022, the Oklahoma State Bureau of Investigation (OSBI) provided OSI with details of a Chevrolet Silverado with Oklahoma Tag Number KCC641 registered to SHELTON. The registration listed the SUBJECT PREMISES as SHELTON's address. On October 17, 2022, OSI drove by the SUBJECT PREMISES and observed a vehicle parked in the rear parking lot matching the description and bearing the license plate number provided by OSBI.

10. On October 20, 2022, OSI observed SHELTON depart his assigned duty location at Tinker Air Force Base, drive to the SUBJECT PREMISES where he entered apartment number 413. Based on information currently available, investigators have no reason to believe that any other persons besides SHELTON live in the SUBJECT PREMISES.

DEFINITIONS

11. The following definitions apply to this Affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Sexual Abuse Material" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed

disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

i. "Peer-to-peer file-sharing" (P2P) is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

j. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

k. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

j. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact

discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND CONCERNING EMAIL

12. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name Gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

13. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

14. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

15. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

16. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically

retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant

insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

18. In my training an experience, I have learned that an email that is sent to a Google subscriber is stored in the subscriber's email mailbox on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

BACKGROUND ON COMPUTERS AND CHILD SEXUAL ABUSE MATERIAL

19. Based on my knowledge, training, and experience in child exploitation and child sexual abuse material investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child sexual abuse material is produced and distributed.

20. Computers basically serve four functions in connection with child sexual abuse material: production, communication, distribution, and storage.

21. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

22. The computer's ability to store images in digital form makes the computer itself an ideal repository for child sexual abuse material. The size of the electronic storage media

(commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

23. The Internet affords collectors of child sexual abuse material several different venues for obtaining, viewing, and trading child sexual abuse material in a relatively secure and anonymous fashion.

24. Collectors and distributors of child sexual abuse material also use online resources to retrieve and store child sexual abuse material, including services offered by Internet Portals such as Google mail and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account such as a Google Drive from any computer with access to the Internet. Evidence of such online storage of child sexual abuse material is often found on the user's computer. Even in cases where online storage is used, however, evidence of child sexual abuse material can be found on the user's computer in most cases.

25. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or

downloaded. Such information is often maintained indefinitely until overwritten by other data. Likewise, devices such as cellular telephones, tablets, and e-readers are also capable of electronic storage as computers.

CHILD SEXUAL ABUSE MATERIAL COLLECTOR CHARACTERISTICS

26. The following indicates characteristics of child sexual abuse material collectors that this Affiant has learned through training, working multiple investigations involving child sexual abuse material, and from other law enforcement officers with a background in child sexual abuse material investigations:

a. The majority of individuals who collect child sexual abuse material are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child sexual abuse material collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child sexual abuse material but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child sexual abuse material often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child sexual abuse material and child erotica as a means of gaining status, trust, acceptance, and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child sexual abuse material maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child sexual abuse material often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child sexual abuse material rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes or other secure location.

CONCLUSION

27. Based on the forgoing, I request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

AUSTINA BLECHA
SPECIAL AGENT
OFFICE OF SPECIAL INVESTIGATIONS

Signed and sworn before me this 29th day of November 2022.

SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE